

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED-PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problems Mailbox.**

THIS PAGE BLANK (USPTO)

09/890002

PCT/AU00/00418



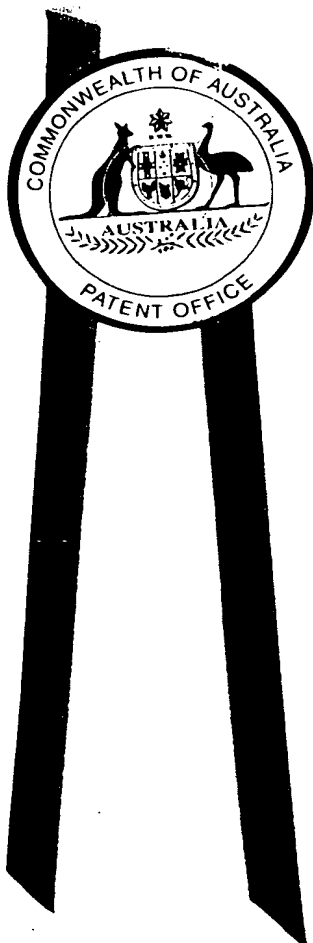
RECD 29 MAY 2000

4

Patent Office
Canberra

I, KIM MARSHALL, MANAGER PATENT ADMINISTRATION hereby certify that annexed is a true copy of the Provisional specification in connection with Application No. PQ 3682 for a patent by FREEONLINE.COM.AU PTY. LIMITED filed on 27 October 1999.

I further certify that the above application is now proceeding in the name of SHARINGA NETWORKS INC. pursuant to the provisions of Section 113 of the Patents Act 1990.



WITNESS my hand this
Eighteenth day of May 2000

KIM MARSHALL
MANAGER PATENT
ADMINISTRATION

**PRIORITY
DOCUMENT**
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)



Sharinga Networks Inc.
~~FREEONLINE.COM.AU PTY. LIMITED~~

A U S T R A L I A
Patents Act 1990

PROVISIONAL SPECIFICATION

for the invention entitled:

"A COMMUNICATIONS NETWORK ACCESS METHOD AND SYSTEM"

The invention is described in the following statement:



A COMMUNICATIONS NETWORK ACCESS METHOD AND SYSTEM

5

The present invention relates to a method and system for accessing a communications network, such as the Internet.

Most Internet users currently connect to the Internet via the equipment of an Internet
10 service provider (ISP). The ISP provides remote access servers (RASs) which are able to
communicate with remote computers of the users using modems and standard telephone lines.
The remote computers and the RASs use standard software that executes a protocol, such as
the point to point protocol (PPP), to allow the users to dial into the RASs and connect to the
Internet. To achieve this, the connection or PPP software on the user's computer requires the
15 user to enter unique authentication data, such as the user's login name and password, and this
is transmitted to the ISP when the software dials and connects to the ISP equipment. If the ISP
equipment determines that the authentication data is valid, the user's computer is connected
and the user is allowed uninhibited access to the Internet. The user is accordingly free to view
any desired web pages using a web browser on the user's computer.

20

The success of web sites on the Internet, particularly from a commercial perspective,
is almost solely dependent on a site's ability to attract traffic to it. For this reason, a number
of well known sites, such as Netscape's home page and the home pages of ISPs have been
reconfigured to operate as communication "portals" to the Internet in the hope that users will
25 continually revert to the sites to determine where to direct their browsers next. A number of
sites have proved to be extremely lucrative, in the same manner as television stations which
are able to attract large numbers of viewers. The current market value of companies such as
Yahoo and Excite, which maintain high traffic volume sites, indicates how lucrative. As ISPs
constitute a first point of connection for most Internet users, any steps or method which an
30 ISP can implement to direct users to particular pages, rather than the user's own default home
page, would be highly desirable. The present invention seeks to provide such method or at
least provide a useful alternative.

In accordance with the present invention there is provided an access system including:
means for connecting a computer device and establishing a connection session for
accessing a network;

switch means having a plurality of access states, one of said access states being
5 assigned to said session for at least part of said session, each access state determining network
traffic receivable by said computer device; and

means for managing said session and assigning at least one of said access states during
said session based on connection data for said session and access requests from said computer
device.

10

Advantageously, the access requests may be requests for data on the Internet, such as
web pages, streaming audio and video, interactive chat sessions, e-mail or FTP sites, and said
access states determine whether the computer device can receive the data. The session
managing means may dynamically assign and adjust the access states during the session. The
15 access system may control the data delivered to the computer device, and an access state may
direct the computer device to a predetermined network location.

The present invention also provides an access system for a communications network,
such as the Internet, including:

20 means for connecting a computer device and establishing a TCP/IP session for access
to the network;

switch means having a plurality of access states, the access states determining the sites
and pages which can be accessed by the computer device during the session; and

means for managing the session to allocate at least one of the access states during the
25 session.

The access states are allocated based on connection data for the session, such as the
IP address for the session and/or profile data held for a user of the computer device. The
session may be allocated a number of access states at respective times during the session based
30 on access requests from the computer device.

Advantageously, the access system may partition the Internet based on respective

access states, which may be allocated to different sessions dynamically. Preferably one of the access states is an affiliate state which restricts access to locations on the network affiliated to a provider of the access system. The access system advantageously may partition or subdivide data provided by third parties on a public network, such as the Internet.

5

The present invention also provides a communications network access method, including:

establishing a TCP/IP session with a computer device; and

10 assigning access states during said session, said access states determining TCP/IP data received by said computer device.

The present invention also provides a communications network access method, including:

connecting a computer device to a communications network;

15 accessing data from affiliate locations on said network without an access charge; and
accessing data from other locations on said network with an access charge.

The present invention also provides a communications network access method, including:

20 receiving a request from a computer device to connect to said network;

connecting said computer device to said network in response to said request;

sending login data to said computer device after said connecting step, said login data being adapted to generate a login display on said computer device allowing entry of unique authentication data by a user of said device;

25 receiving said unique authentication data entered on the computer; and

allowing said user to access said network using said computer device when said authentication data is validated.

30 Preferably said method includes accessing profile data for said user after said allowing step and controlling access to said network using said profile data. Advantageously, said method may include having a set of access profiles or states encoded in a switch, and said profile data accessed for said user represents one of said encoded profiles or states.

Advantageously, the login display may include advertising material and links to particular locations on the communications network. Advantageously, the communications network may be the Internet and said login data represents a login web page sent to said computer device after connecting to the network. Advantageously, said request receiving and
5 connecting steps may be executed using standard communication protocols, such as PPP, and a modem of the computer device and a RAS of the network. Advantageously, the steps of the method may be executed by equipment of an ISP.

The present invention also provides a communications network access system,
10 including:

means for receiving a request from a computer device to connect to said network and for connecting the computer device to the network in response to the request;

means for sending login data to the computer device after it is connected to the network, said login data being adapted to generate a login display on the computer device
15 which allows entry of unique authentication data by a user of the device; and

means for receiving said unique authentication data entered by the user and for allowing the user to access the network using the computer device on determining that the authentication data is valid.

20 Advantageously, the receiving and connecting means may include a RAS. The sending means may include a web server, and the receiving and allowing means may include, the web server and a user database.

The present invention also provides a communications network access method,
25 including:

sending a request from a computer device to connect to a communications network, and being connected to the network in response to the request;

receiving login data after being connected;

generating a login display on the computer device, based on the login data, said
30 display allowing entry of unique authentication data;

sending unique authentication data entered on the computer device to the network; and obtaining access to the network after said authentication data is validated.

A preferred embodiment of the present invention is hereinafter described, by way of example only with reference to the accompanying drawings, wherein:

Figure 1 is a block diagram of a preferred embodiment of a communications network access system;

5 Figure 2 is a block diagram of a server system of the access system;

Figure 3 is a flow diagram of a communications network access method of the access system;

Figure 4 is a diagram of a login page of the system and method; and

Figure 5 is a diagram of a customised home page of the system and method.

10

A communications access system, as shown in Figure 1, includes a plurality of remote access servers (RASs) 4, a layer four or higher switch 6, a database server 8, a web server system 10 and a router 12. The RASs 4 are provided to allow the computers 14 of remote users to dial into the system using standard telecommunication lines and modems and connect to the input ports of the RASs 4, respectively. On connection to a port of a RAS 4, the RAS 4 and the user's computer 14 establish a unique TCP/IP session and the IP traffic for that session is switched by the switch 6. Once the user is authenticated or approved, as described below, the user's computer 14 is allowed to access requested data on the Internet 16. The web server system 10 is used to control pages presented to a user 14 connected to the RAS 4 and handle authentication using a member profile database maintained on the database server 8, as described below. A RADIUS (Remote Authentication Dial In User Service) authentication server 11 is also provided for use in authentication. As far as the user 14 is concerned, the equipment 4, 6, 8, 10, 11 and 12 of the access system is part of the Internet. The equipment 4 to 12 includes standard commercially available hardware and basic database, web server and Internet access software which is known to those skilled in the art and is used in the access systems of most ISPs. The equipment 4 to 12 also includes unique program code to manage and control each session, as discussed below. The layer four or higher switch 6 is another exception. The switch 6 is normally used by ISPs to balance the traffic handled by the RASs 4. An example of a suitable layer four switch is the 700 Series Switch™ produced by Alteon WebSystems Inc. The access system differs from that offered by ISPs, as described below, in that the layer four switch 6 is used to connect users to the web server system 10 and control access to the Internet 16 for the users 14 on the basis of a limited number of access states

encoded in the switch 6.

The switch 6 controls access to the Internet 16 by assigning an access state to each TCP session, as identified by a respective IP address. The states are each defined by one or more access rules which are encoded in the switch 6. The rules define how the switch 6 is to direct IP traffic by executing pattern matching on the received traffic. For example, the states may include a login state, a portal state, a general state, an affiliate state, a registration state, and an allow state, as described below. A rule, for example, may be take access to a first URL and redirect to a second URL or the rules may allow or deny access to a predetermined set or list of URLs. The state assigned to a given IP address is controlled by a login system 20, as shown in Figure 2. The web server system 10 includes the login system 20 and a web server 22, running Apache™, which maintains web pages for the access system.

When the user 14 wishes to connect to the Internet using the access system, the user 14 dials into the system using standard PPP software and is allocated a port at the RAS 4 which answers the call. On connecting to a RAS 4, the user 14 is assigned an IP address for the IP session. The IP address is allocated from an IP address pool which depends on the number which the user dialled to connect to the RAS 4. For example, the user may have a dial-in number which provides the user with free access to Internet web sites as part of a promotion, and the user 14 is assigned an IP address and port which signifies to the switch 6 that all traffic at that IP address is to be switched directly to the router 12 and out to the Internet 16. This would occur with all IP addresses within this pool being allocated to the affiliate state of allow state of the switch 6, described below. Every other IP address assigned by the RASs 4 is initially allocated to a login state of the switch until the state is changed by the login system 20. Traffic with IP addresses assigned to the login state is all redirected to the login system 20 by switch 6.

The login system 20, as shown in Figure 2, includes a RADIUS accounting server 30, a login server 32, a session coordinator 34, individual session managers 36, an authentication client 38, a redirector server 42 and a plan manager 44. The components 30 to 44 are all software components, but can if desired be partly or entirely replaced by application specific integrated circuits (ASICs). The login system 20 is configured to handle three different

. 8 .

authentication scenarios:

- (i) Legacy authentication using the RADIUS authentication server 11.
- (ii) Authentication using a login display, e.g. browser based authentication.
- (iii) No authentication required.

5

For the first scenario, the user 14 dials into the RASs 4 using standard PPP software and provides a username and password. Based on the dial in number used and the configuration of the PPP software, the RAS port assigned to handle the call will direct the data provided to the RADIUS authentication server 11 to authenticate the user based on the PPP username and the password. Once authenticated, the RADIUS authentication server 11 returns a connect status message to the RAS 4 and an IP address is assigned to the user. Based on the IP address, the switch 6 forwards from the RAS 4 the connect status message, the username, calling line identification and the IP address to the login system 20. This data is processed by the RADIUS accounting server 30 which acknowledges the new connection for the IP address and accesses the database server 8 to record the connection time for the user. The RADIUS accounting server 30 acknowledges and monitors all connections and disconnections for IP addresses, and issues connection and disconnection messages to other components in the access system. The session coordinator 34 uses the connection data, together with profile data accessed from the member profile database for the user 14, to create an instance of a session manager 36 for the connection. Session managers 36 are created for each connection or session, respectively, and provide instructions to the redirector server 42 to control the state at the switch 6 for the session.

A session manager 36 controls the traffic which the user can receive during the session by controlling the state of the switch for the user's IP address. The state control is executed on the basis of the user's member profile held in the member profile database of the server 8. The profile specifies which one of a limited number of access profiles the user belongs to. The access profiles each contain data which defines the access states that the user is able to enter. The different access states are encoded in the switch 6. On authentication of a TCP/IP session the session manager 36 for the session instructs the redirection server 42 to store data in the switch 6 indicating which one of the access states apply to the session. For example, during authentication the session is in a login state and can change to a general state or

affiliate state once authentication has been completed.

In the second authentication scenario, the access system executes browser based authentication using the access procedure shown in Figure 3. The user is able to connect to the Internet by simply dialling into the access system using standard PPP software, at step 22, and the RASs 4 will automatically connect the user 14 without requiring the entry of any username or password. The user is automatically connected, an IP address assigned and a TCP session established, when the user dials into a port of a RAS 4 using predetermined call numbers. The system informs the user's computer 14 of the connection and the PPP software will display for the user the fact that the connection has been established and any other details associated with the connection, such as the data rate. The IP address is assigned from an address pool for immediate connection.

Once the user is connected to the access system the switch 6 determines whether the user's machine 14 is requesting connection to another computer on the Internet 16, at step 24. The request for example, may be simply to the user's default home page when the user opens a web browser of the computer 14. The switch 6 then determines, at step 26 by checking a stored flag representing the switch state for the IP address, whether the user has been authenticated and that the state is not the login state. If the switch 6 is in the login state, the switch 6 connects the user 14 to a login page on the web server 22, and the login system 20 executes a login process 28. The login process 28 is similar to that for legacy authentication, in that the RAS accounting server 30 acknowledges that connection has occurred and a new session has been established for the IP address. Data for the session is passed to the session coordinator 34 to create an instance of a session manager 36 for the session. Based on the IP address, however, the session manager 36 determines that the user needs to be authenticated using browser based authentication and accordingly waits for the login server 32 to receive from the web server 22 details submitted on the login page shown in Figure 4. The login page presents the user with a number of options, which includes executing a registration process to become a new registered user, entering a username and password if already registered, or accessing help pages stored on the server 22. The page also includes a number of banner advertisements which may include links to other pages or web sites. To gain general access to the Internet 16, however, the user must enter a valid username and password combination

which is authenticated by the login system 20. The login page allows the user to enter a username and password combination and then send the combination for authentication by clicking on the "sign in" button. Alternatively the combination may already be stored on the computer 14 by the user. The username and password combination is received by the session manager 36 for the session and the combination is forwarded to the authentication client 38. The authentication client 38 passes the combination to an authentication daemon 40 running on the database server 8. The authentication daemon checks the combination against stored combinations for users to determine if it is valid, identify the user and access the unique member profile for the user from the database server 8.

10

In the third authentication scenario, no authentication is required. In this scenario the user is allocated a telephone number to dial in on which corresponds to no authentication. The user is automatically connected, as for browser based authentication, and assigned an IP address from a pool for no authentication. Operation proceeds as described above for browser based authentication, except that the session manager 36 does not revert to the authentication client 38 to authenticate the user based on a username and password combination. The user is simply authenticated automatically by the session manager 36.

Once the user has been authenticated, either by the login process 28 or using the RADIUS server 11, an individual session manager 36 uses the member profile data for the user to compile and send a customised home page, as shown in Figure 5 to the user 14. The customised home page may also include banner advertisements, in the same manner as for the login page. The session manager 36 instructs the redirector server 42 to change the state of the switch 6 to a portal state, after authentication, which directs the switch to connect to the URL for the customised home page or portal shown in Figure 5. Details concerning the user and customised home page data from the member profile are passed by the session manager 36 to the login server 32 for access by the Apache server 22 which controls compilation of the customised home page. Subsequently, the session manager 36 instructs the redirector server so as to divert the switch to one of the browsing states, either an affiliate state or a general state. For browser based authentication, as shown in Figure 3, the login authentication process is managed using the web browser of the user's machine 14, rather than the PPP software, and operation returns after the login process 28 to step 24. Accordingly, once the

user reverts to step 24 and is determined at step 26 as having been authenticated, the switch 6 determines at step 30, on the basis of the access state for the session, whether the user is allowed to access a requested computer or service. If so, the user is granted access to the computer or service on the Internet 16 at step 32. If not, the user 14 is advised at step 34 of the access denial. The access denial can be communicated by connecting the user to a denial page of the Apache server 22.

A user 14 having a session which is in the affiliate state is allowed access, at no charge, to sites maintained by affiliates of the provider of the access system. The affiliate sites may be maintained on the Apache server 22 or on other servers of the Internet 16. The affiliate sites are all identified by URLs in the rules of the affiliate state. The affiliate sites can also be accessed using the links provided in the web pages of Figures 4 and 5. The rules for the affiliate state specify that access is denied to any URLs which do not belong to the affiliate sites. If however a user has a member profile that allows access to other sites on the Internet, the user is able to move to the general state. For these users, when a request is made to access a site other than an affiliate site, the user's browser is redirected by the switch 6 to an interim blank page on the Apache server 22 while the session manager 36 determines whether to instruct the redirector server 42 to change the state of the switch to the general state. The interim blank page contains code to trap the requested URL and pass the URL and a message to the login server 32 advising that the user is attempting to move from the affiliate state to the general state. This message is passed to the session manager 36, on the basis of the IP address, and the session manager 36 accesses the member's profile. If the session manager 36 determines on the basis of the profile that the user 14 is allowed to move the general state, a message is sent to the redirector server 42 to change the state of the switch to the general state for the session. A message is also sent from the manager 36 to the login server 32 advising that the user 14 is allowed to move to the trapped URL. The login server 32 sends a message to the Apache server 22 to forward the user 14 from the interim page to the page of the requested trapped URL. If access is denied, the URL of a denied page is used to substitute the trapped URL at the login server 32, and the user 14 is forwarded to the denial page.

Other access states are the registration state and the allow state. A session manager 36

will instruct the redirector server 42 to enter the switch into the registration state for a session when a user sends a message indicating they wish to register with the access system. This may be done when, for example, the user selects the registration option on the login page of Figure 4. In the registration state the switch 6 redirects the user 14 to registration pages on the Apache server 22 and the login system 20 collects the requested details on the pages from the user 14 for the user file in the data base server 8. A session manager 36 will instruct the redirector server to cause the switch 6 to enter the allow state when the IP address indicates that the user 14 is to be provided with unrestricted access to the Internet 16 without any monitoring or charge.

10

When the session is disconnected, the RAS 4 communicates disconnection to the RADIUS accounting server 30, which in turn advises the session manager 36. The manager 36 instructs the redirector server 42 to change the state of the switch to the login state for the IP address of the disconnected session.

15

The manner in which the user is charged is controlled by a plan manager 44 that is accessed by the session manager 36. The plan manager 44 maintains different charging plans which can be applied to users. For example, all users would not be charged for access to affiliate sites, but the rate of charge may differ for accesses when in the general state. For instance, users may be allocated a predetermined period of free access for pages to the general state and then charged at a set rate thereafter. The plan manager specifies the times and rates for the different plans, and this is accessed by the session managers 36 which monitor the time a user spends in different access states. The ultimate charge for a session is compiled by the session managers 36 and then stored against the user's file in the database server 8.

25

The access method and system are particularly advantageous as they allow ISPs, at least initially, to dynamically control the pages viewed by a user. As a minimum, the user must, and cannot avoid, viewing the login or customised home page, as these are an integral part of the login process. This allows the ISP to present advertising information, and in particular present targeted advertising information based on the user's profile, which the ISP can guarantee that all of its users will not be able to avoid. The login and customised home pages therefore act as an entry portal for all users.

By also allowing all users to connect to the system, including users which are not registered, the ISP is able to present and provide free access to selected and predetermined Internet content and services. For example, the login page may include links to certain web pages that provide banking, stock trading or home shopping, and the user will not have to pay
5 any fees to the ISP to access these pages. This allows the ISP to act as a free content provider for certain content, whilst charging a user to access other data on the Internet. To provide information to advertisers associated with the free content, the ISP can, if desired, still require and obtain certain information on and from users before providing the free content, and monitor their access.

10

Encoding the access states in the switch 6 also allows the ISP to restrict or allow access to selected content or services on the Internet, such as sports betting, adult orientated content or children's content.

15 Many modifications will be apparent for those skilled in the art without departing from the scope of the present invention as hereinbefore described with reference to the accompanying drawings.

20

DATED this 27th day of October, 1999

FREEONLINE.COM.AU PTY. LIMITED

25 By its Patent Attorneys

DAVIES COLLISON CAVE

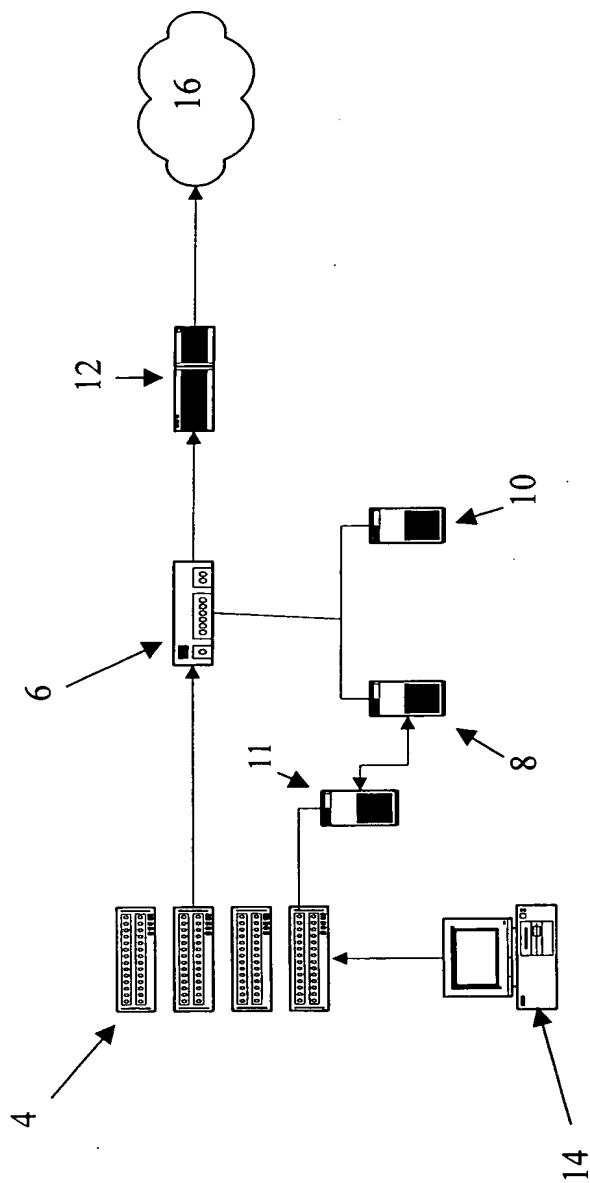


Figure 1

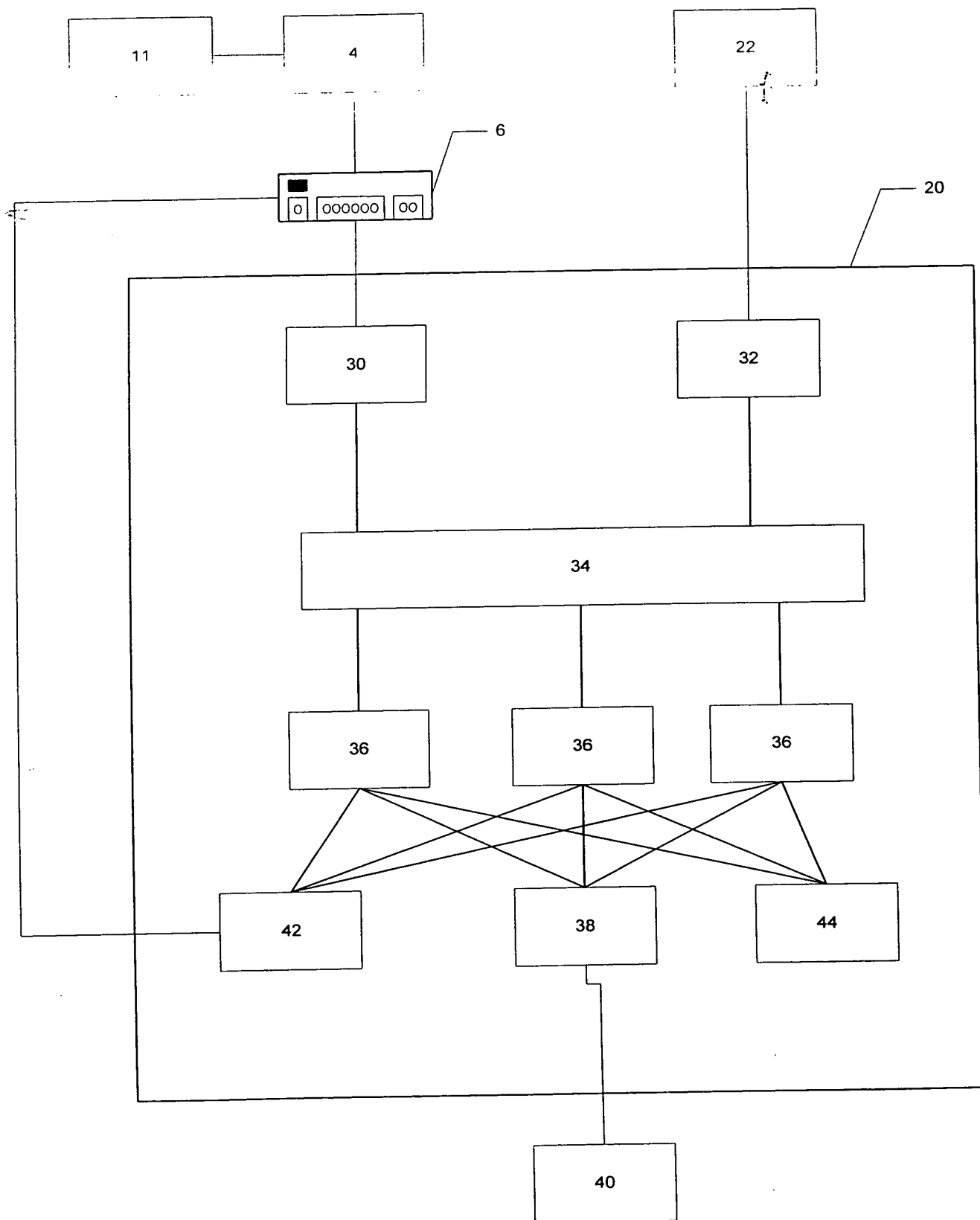


Figure 2

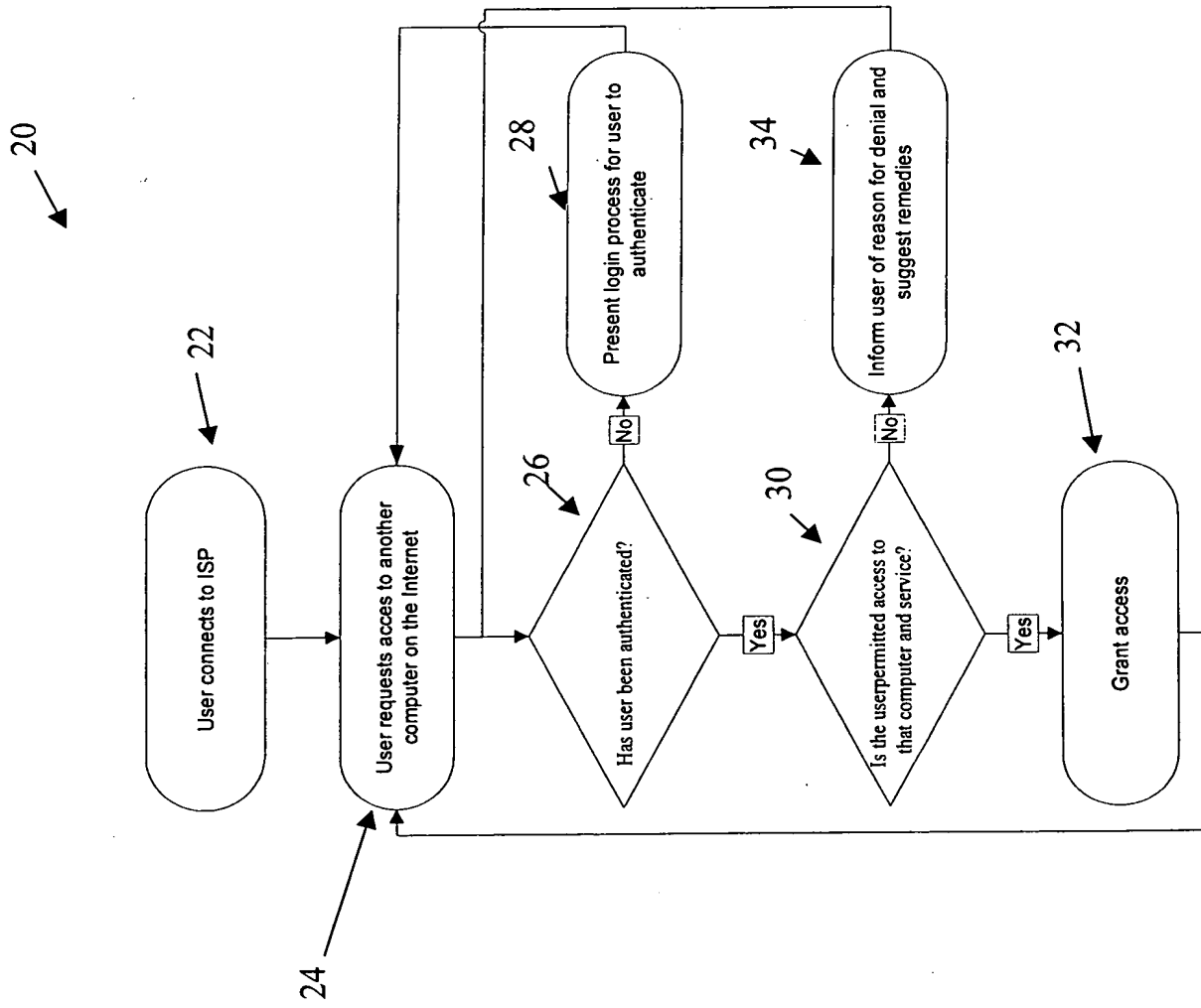


Figure 3

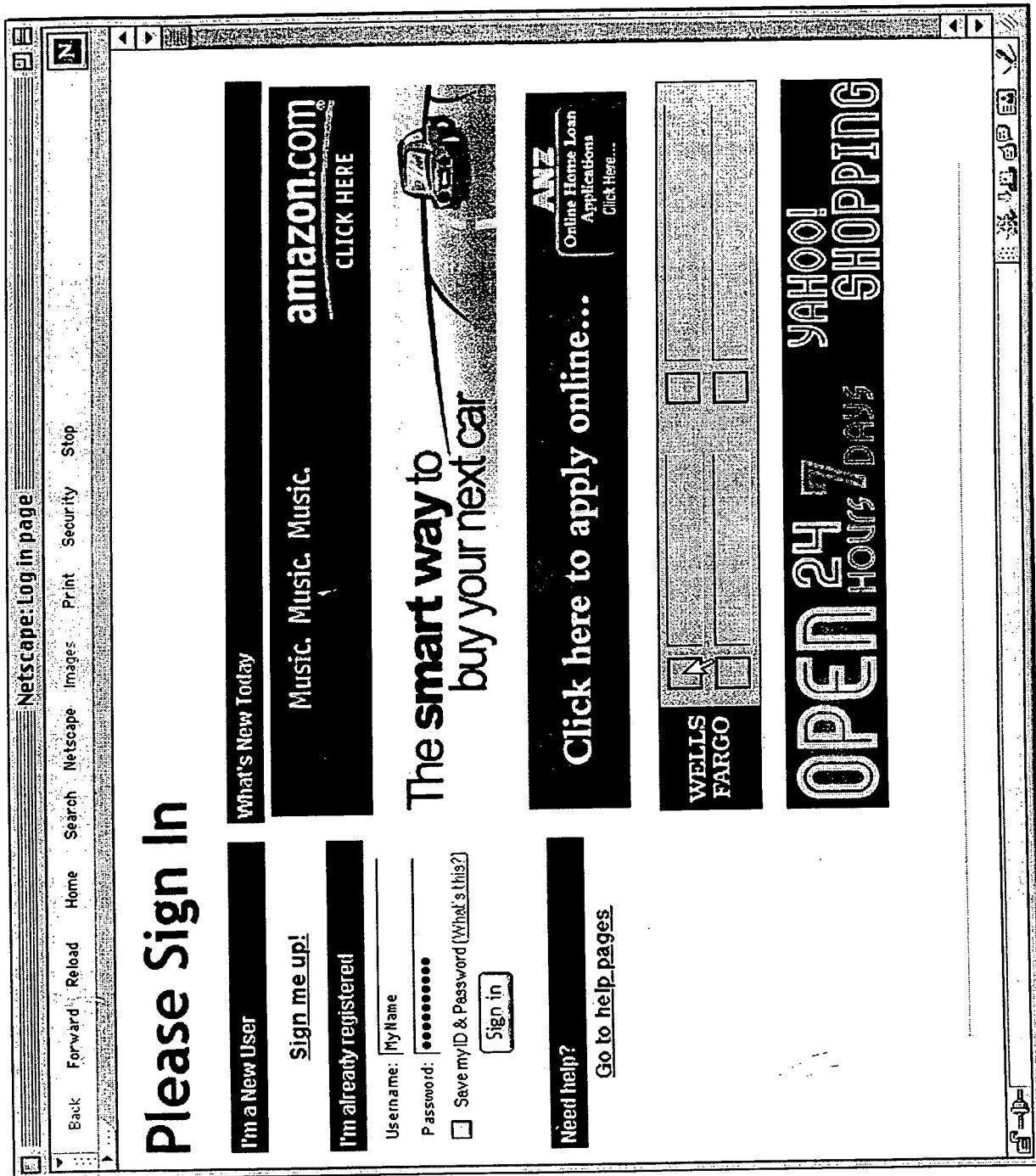


Figure 4

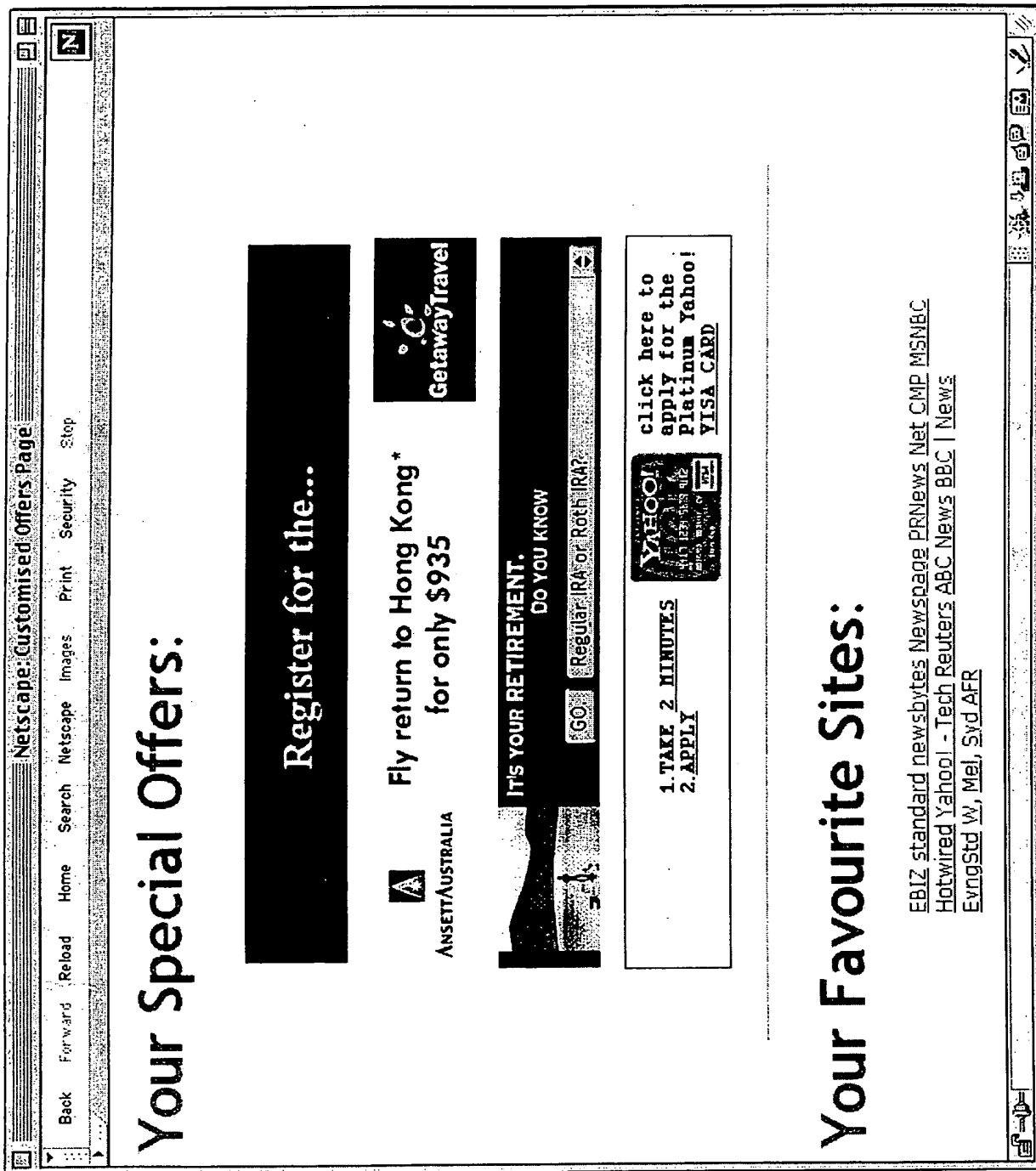


Figure 5

THIS PAGE BLANK (USPTO)